Claims

1. An cryptographic processing apparatus for performing Feistel-type common-key-block cryptographic processing, having

a structure that repeatedly executes an SPN-type F-function having a nonlinear conversion section and a linear conversion section over a plurality of rounds, wherein

each of the linear conversion section of an F-function corresponding to each of the plurality of rounds is configured to perform linear conversion processing of an input of n bit outputted from each of the m nonlinear conversion sections, totally mn bit, as linear conversion processing that applies a square MDS (Maximum Distance Separable) matrix, at least in the consecutive odd-numbered rounds and in the consecutive even-numbered rounds, different square MDS matrices L_a, L_b are applied, and

a matrix composed of m column vectors selected arbitrarily from column vectors constituting inverse matrices L_a^{-1}, L_b^{-1} of the square MDS matrices is linearly independent.

2. The cryptographic processing apparatus for performing the Feistel-type common-key-block cryptographic processing according to claim 1, wherein

a matrix composed of m column vectors selected arbitrarily from column vectors constituting the inverse matrices L_a^{-1}, L_b^{-1} is a square MDS matrix.

3. The cryptographic processing apparatus for performing the Feistel-type common-key-block cryptographic processing according to claim 1, wherein

an algorithm of the Feistel-type common-key-block cryptographic processing is a cryptographic algorithm of round number 2r, and

the linear conversion section of the F-function is configured to execute linear conversion applying q kinds of different square MDS matrices (2 ≤ q <r) sequentially and repeatedly in all of the r even-numbered rounds and in all of the r odd-numbered rounds.

4. The cryptographic processing apparatus for performing the Feistel-type common-key-block cryptographic processing according to claim 1, wherein

each of the plurality of different square MDS matrices to be applied in the linear conversion section of the F-function is a square MDS matrix that is composed of m column vectors selected arbitrarily from column vectors constituting the plurality of square MDS matrices and is linearly independent.

5. The cryptographic processing apparatus for performing the Feistel-type common-key-block cryptographic processing according to claim 1, wherein

each of the plurality of different square MDS matrices to be applied in the linear conversion section of the F-function is a square MDS matrix such that a matrix composed of m column vectors selected arbitrarily from column vectors constituting the plurality of square MDS matrices is also a square MDS matrix.

6. The cryptographic processing apparatus for performing the Feistel-type common-key-block cryptographic processing according to claim 1, wherein

each of the plurality of different square MDS matrices to be applied in the linear conversion section of the F-function

is made up of a matrix composed of row vectors extracted from a matrix M' that is composed of row vectors selected from a square MDS matrix M including all elements constituting the plurality of square MDS matrices.

7. An cryptographic processing method for performing Feistel-type common-key-block cryptographic processing, comprising the steps of:

executing an SPN-type F-function for performing nonlinear conversion processing and linear conversion processing repeatedly over a plurality of rounds; and

in the conversion processing of an F-function corresponding to each of the plurality of rounds, performing linear conversion for n bit outputted from the m nonlinear conversion sections, totally mn bit, as linear conversion processing applying square MDS (Maximum Distance Separable) matrices; wherein

linear conversion processing with square MDS matrices such that at least in the consecutive even-numbered rounds and in the consecutive odd-numbered rounds different square MDS matrices L_a, L_b are applied, and a matrix composed of m column vectors selected arbitrarily from column vectors constituting the inverse matrices L_a^{-1}, L_b^{-1} of the square MDS matrices is linearly independent and makes up a square MDS matrix.

8. The cryptographic processing method for performing the Feistel-type common-key-block cryptographic processing according to claim 7, wherein

linear conversion processing by square MDS matrices such that a matrix composed of m column vectors selected arbitrarily from column vectors constituting the inverse matrices L_a^{-1}, L_b^{-1} is a square MDS matrix.

9. The cryptographic processing method for performing the Feistel-type common-key-block cryptographic processing according to claim 7, wherein

an algorithm of the Feistel-type common-key-block cryptographic processing is a cryptographic algorithm of round number 2r, and

the linear conversion processing of the F-function executes linear conversion processing sequentially and repeatedly applying q kinds of different square MDS matrices ($2 \leq q < r$).

10. The cryptographic processing method for performing the Feistel-type common-key-block cryptographic processing according to claim 7, wherein

each of the plurality of different square MDS matrices to be applied to the linear conversion processing of the F-function is such that a matrix composed of m column vectors selected arbitrarily from column vectors constituting the plurality of square MDS matrices is linearly dependent and makes up a square MDS matrix.

11. The cryptographic processing method for performing the Feistel-type common-key-block cryptographic processing according to claim 7, wherein

each of the plurality of different square MDS matrices to be applied to linear conversion processing of the F-function is a square MDS matrix such that a matrix composed of m column vectors selected arbitrarily from the column vectors constituting the plurality of square MDS matrices becomes a square MDS matrix.

12. The cryptographic processing method for performing the Feistel-type common-key-block cryptographic processing according to claim 7, wherein

each of the plurality of different square MDS matrices to be applied to the linear conversion processing of the F-function is made up of a matrix composed of column vectors extracted from a matrix M' composed of row vectors selected from a square MDS matrix M that includes all elements constituting the plurality of square MDS matrices.

13. A computer program of performing the Feistel-type

common-key-block cryptographic processing according to claim 7, comprising the step of:

executing an SPN-type F-function for performing nonlinear conversion processing and linear conversion processing over a plurality of rounds, wherein

the linear conversion processing of the F-function corresponding to each of the plurality of rounds is a linear conversion step of performing linear conversion processing for n bit outputted from the m nonlinear conversion sections, totally mn bit, as linear conversion processing applying a square MDS (Maximum Distance Separable) matrix, and

in the linear conversion step, linear conversion processing by square MDS matrices is executed

in such a way that at least in the consecutive even-numbered rounds and in the consecutive odd-numbered rounds, different square MDS matrices are applied, and a matrix composed of m column vectors selected arbitrarily from column vectors constituting inverse matrices L_a^{-1}, L_b^{-1} of the square MDS matrices is linearly independent.